

From: "Riedl, Daniel J. (USAOHN)" <DRiedl@usa.doj.gov>

To: "Ian Friedman" <inf@fanlegal.com>

Cc: "Bennett, Mark S. (USAOHN)" <MBennett3@usa.doj.gov>

Subject: Re: Davis Lu

Date: Thu, 28 May 2020 15:29:37 -0000

Importance: Normal

Inline-Images: Outlook-e01uhgj2.png

Mr. Friedman,

Thank you for following up in the matter of your client, Davis Lu. We are nearly finished with the investigation. I will be sending an email shortly with a .zip attachment. **The passphrase for the .zip file is DavisLu2020!** The zip file contains several reports from the FBI's investigation into Lu. We are waiting on additional reports which are written but need to be submitted and approved by supervisors before they become part of the casefile. Although I haven't reviewed those reports yet, I will attempt to summarize the most relevant results from the investigation.

The FBI, Eaton and Dassault (the third party vender responsible for the server at issue) identified and reviewed the code that caused the Eaton servers to crash. There are multiple indicators in the code, on Lu's laptop and on Eaton's network that this code was written and executed by Lu. Further, Lu admitted to FBI SA Monica Hantz that he wrote the code. Neither Dassault, Eaton employees or the FBI computer scientist see any legitimate purpose for these pieces of code. They believe the code was written for the sole purpose of causing the logon server to crash and deny other employees access to the network. Lu's coworkers report Lu is an experienced programmer and would not have created an infinite loop in a program unintentionally. Lu was not asked to write this code or to conduct tests on the server. According to Eaton, Dassault and the FBI computer scientist, the code doesn't test anything. It is a simple piece of code that creates an infinite loop that crashes the logon server. This is not something that any Eaton programmer would ever be asked to do or think it a good idea to attempt on his or her own initiative.

Additional malicious code was found on the work laptop assigned to Lu. One program would have caused the server to check whether Lu's account was active. If the account was not active, the code would have prevented others from logging onto the servers. Essentially, this would have locked everyone out of the development server unless Lu logged on. Again, Lu was not asked to write this code and there is no legitimate purpose for its existence. While there is no evidence this code was deployed on Eaton's servers, the fact that Lu wrote it is further proof that Lu intended to deny other employees access to Eaton's servers.

Eaton is in the process of quantifying the loss caused by Lu's malware. Currently, Eaton estimates their damages at \$387,500. This number is subject to change.

Our investigation is nearly complete and I believe the evidence is sufficient to pursue charges against Mr. Lu. Please let me know if Mr. Lu would like to explore a pre-indictment information and plea agreement. I ask that you give me a preliminary answer by Friday, June 12.

As always, don't hesitate to contact me or AUSA Mark Bennett with any questions.

Sincerely yours,
Dan Riedl

Daniel J. Riedl
Chief, National Security and Cyber Unit
Northern District of Ohio
801 West Superior Avenue, Suite 400
Cleveland, OH 44113-1852
(o) 216-622-3669
(m) 216-338-4883



CONFIDENTIAL U.S. ATTORNEY E-MAIL COMMUNICATION

The information contained in this electronic message, and any and all accompanying documents constitutes confidential information and may be privileged. This information is the property of the U.S. Attorney's Office. If you are not the intended recipient of this information, any disclosure, copying, distribution, or the taking of any action in reliance on this information is strictly prohibited and may be unlawful. If you are not an intended addressee, or received this message in error, please notify us immediately at the above number to make arrangements for its return to us.

From: Ian Friedman <inf@fanlegal.com>
Sent: Tuesday, May 26, 2020 4:04 PM
To: Riedl, Daniel J. (USAOHN) <DRiedl@usa.doj.gov>
Subject: Davis Lu

Hi Dan,

I hope that you are well. I am just checking in on the Lu investigation. At your convenience, please let me know where it stands. Thank you Dan.

Ian

Ian N. Friedman, Esq.
Friedman & Nemecek, L.L.C.
The IMG Center
1360 E. 9th Street, Suite 650
Cleveland, Ohio 44114
T: 216.928.7700
E: inf@fanlegal.com
W: www.fanlegal.com
TW: @iannfriedman